Complexity Theory Preliminaries

Charles E. Hughes

cs.ucf.edu/~ceh

cs.ucf.edu/courses/cot6410/Spring2023/ COT6410Spring2023.html

Sets, Sequences, Relations, Cardinality, Proofs

This is review material.

I will not explicitly discuss these concepts and processes in class.

Sets

- *Sets* are unordered collections of distinct objects.
- Sets can be defined or specified in many ways:
  - By explicitly enumerating their members or elements
    e.g. S = { a, b, c}
    Note: If S' = { b, c, a}, then S and S' denote the same set (that is, S' = S)
  - By specifying a condition for membership
    S = { x $\in \Delta$ | P(x) }, reads "S is the set of all x in Δ such that P(x) is true"
    P is called a "predicate" (a function from set Δ to {true, false})
    E.g. S = { x $\in N$ (natural numbers) | x is a prime number }
- The empty set is denoted, $\varnothing$, and is the set with no members; that is,
  $\varnothing$ = { }. Also, the predicate, x $\in \varnothing$ is always false!
- *Multisets* or *Bags* are unordered collections of objects where we keep
  track of repeated elements (usually with a count per element)

More on Sets

- If $S \neq \varnothing$, then there exists an x for which $x \in S$ is true; this predicate is read "x is an element of S" or "x is a member of S". The symbol "$\in$" denotes the member relation. $x \notin S$ is true when x is not in S.

- We use normal set operation of union ($A \cup B$), intersection ($A \cap B$) and complement ~A (usually A with a bar on it).

- If A and B are sets, then we write "$A \subseteq B$" to mean that A is a subset of B. This means that for all $x \in A$, $x \in B$. Or, $\forall x [x \in A \Rightarrow x \in B]$.

- The expression, "$A \subsetneq B$" means that A is a proper subset of B. Mathematically, $\forall x [x \in A \Rightarrow x \in B]$ and $\exists y [y \in B \text{ and } y \notin A]$

- The cross (Cartesian) product of two sets A and B is denoted, $A \times B$, and is the set defined as follows: $A \times B = \{ (a,b) \mid a \in A \text{ and } b \in B \}$. "(a,b)" is an expression composed from elements, a,b, selected arbitrarily from sets A and B, respectively. If $A \neq B$, then $A \times B \neq B \times A$.
  Note: (a,b) is a sequence not a set. See next slide.

Sequences

- While sets have no order and no repeated elements, *sequences* have order and can contain repeats at differing positions in the order.
    - The set {5,2,5} = {5,2} = {2,5}
    - The sequence (5,2,5) ≠ (2,5,5) ≠ (5,5,2) ≠ (5,2) ≠ (2,5)
- Actually, there is a notion of a *multiset* or *bag* that we sometimes use. It has no order, but repeated elements are allowed. Since position is irrelevant, we just record each unique elements with a count.
- We can talk about the *k-th element* of a sequence, but not of a set or multiset.
- Finite sequences are often called *tuples*. Those of length k are *k-tuples*. A 2-tuple is also called a *pair*.

Relations

- A *relation*, r, is a mapping from some set A to some set B;

  We write, r: A $\rightarrow$ B, and we mean that r assigns to every member of A a subset of B; that is, for every a $\in$ A, r(a) $\subseteq$ B and r(a) $\neq$ $\varnothing$.

  A relation, r, can also be defined in terms of the cross product of A and B:
  r $\subseteq$ A $\times$ B such that for every a $\in$ A there is at least one b $\in$ B such that (a, b) $\in$ r.

- We say that a relation, r, from A to B is a *partial relation* if and only if for some a $\in$ A, r(a) = $\varnothing$ = { }.

More on Relations

- A *predicate* or *property* is a function with range {TRUE, FALSE}

- A property with a domain of n-tuples A^n is an n-ary relation

- Binary relations are common, and like binary functions, we use infix notations for them

- Let R be a binary relation on A^2. R is:

  - *Reflexive* if $\forall\, x \in a,\; x\, R\, x$

  - *Symmetric* if $x\, R\, y \rightarrow y\, R\, x$

  - *Transitive* if $(\, x\, R\, y,\, y\, R\, z\,) \rightarrow x\, R\, z$

  - An *equivalence* relation if it is reflexive, symmetric and transitive

Functions

- Functions are special types of relations. Specifically, a relation f: A$\rightarrow$ B, is said to be a (total) function from A to B if and only if, for every a $\in$ A, f(a) has exactly <u>one element</u>; that is, |f(a)| = 1.

- If f is a *partial* function from A to B, then f may not be defined for every a $\in$ A. In this case we write |f(a)| $\leq$ 1, for every a in A; note that |f(a)| = 0 if and only if f(a) = $\emptyset$, and we say the function is *undefined* at a.
  Note: Text calls the set of possible inputs a function's *domain*. We will often use domain for the set of input values on which f is defined, referring to the input set as the universe of discourse. If a function is *total* (defined everywhere) then there is no terminology difference.

- A function, f, is said to be one-to-one (1-1) if and only if x $\neq$ y implies f(x) $\neq$ f(y). A total function that is one-to-one is sometimes called an *injection.*

- A function, f: A$\rightarrow$ B, is said to be onto if and only if for every y $\in$ B there is an x $\in$ A such that y = f(x).
  Note: technically we should write {y} = f(x), since functions are relations, however, the more convenient and less baroque notation is used when dealing with functions. Total functions that are onto are called *surjections*. Ones that are 1-1 and onto are called *bijections*.

Ordinal and Cardinal Numbers

Definition. *Ordinal numbers* are symbols used to designate relative position in an ordered collection. The ordinals correspond to the natural numbers: 0, 1, 2, … The set of all natural (ordinal) numbers is denoted, $\textbf{\textit{N}}$.
(Note: We adopt the notation that 0 is a natural number.)

A fundamental concept in set theory is the size of a set, S. We begin with a definition.

Definition. Let S be any set. We associate with S, the unique symbol |S| called its *cardinality*. Symbols of this kind are called *cardinal numbers* and denote the size of the set with which they are associated.
$|\varnothing| = 0$ (the cardinal number defining the size of the empty set is the ordinal, 0)
If S = {0, 1, 2, 3, …, n-1}, for some natural number n>0, then |S|=n.
To summarize, the cardinality of any <u>finite set</u> (including the empty set) is simply the ordinal number that specifies the number of elements in that set.

More on Cardinality

To determine the relative size of two sets, we need the following definitions:

Definition. If A and B are two sets, then $|A| \leq |B|$ if and only if there exists an injection, f, from A to B; f is a 1-1 function from A <u>into</u> B.

Definition. If A and B are two sets, then $|A| = |B|$ if and only if $|A| \leq |B|$ and $|B| \leq |A|$. We may also say that $|A| = |B|$ if and only if there is a bijection, f, from A to B; f is a 1-1 function from A <u>onto</u> B.

Definition. If A and B are two sets, then $|A| < |B|$ if and only if $|A| \leq |B|$ and $|A| \neq |B|$.

Definition. A set S is said to be <u>finite</u> if and only if $|S| \in N$, otherwise, S is said to be <u>infinite.</u> A set S is said to be <u>countable</u> if and only if S is finite or $|S| = |N|$; otherwise S is said to be <u>uncountable.</u> We discuss cardinality in more details later.

Infinities

By the definitions above, there are many infinite sets with which you are familiar.

For example:
N (the set of Natural numbers), Z (the set of Integers), Z^+ (the set of Positive Integers), Q (the set of Rational numbers) and R (the set of Real numbers).

But, are all these infinite sets the same size??

Brash statement: $|N| = |Z^+| = |Z| = |Q| < |R|$.

Power Set

Definition. Let S be a set, then the power set of S, denoted $\mathcal{P}(S)$ or 2^S, is defined by

$\mathcal{P}(S) = \{\ A\ |\ \ A \subseteq S\ \}$.

Examples.
$\mathcal{P}(\varnothing) = \{\varnothing\}$,
$\mathcal{P}(\{1,2,3\}) = \{\varnothing, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\}$

$\mathcal{P}(N) =$ $\{\varnothing, \{0\}, \{1\}, \{2\}, \{3\}, \ldots$
$, \{0,1\}, \{0,2\}, \{0,3\}, \ldots$
$, \{0,1,2\}, \ldots$
$\ldots \{\ N\ \}\ \}$

Cantor and Infinities

The previous "brash" statement suggests there are at least two infinite cardinals, $|N|$ and $|R|$. Furthermore, $|N|$ is a countable cardinal and $|R|$ is an uncountable cardinal. In fact, there are infinitely many distinct cardinal numbers representing infinite sets!

In addition to these facts, Cantor proved that there is a smallest infinite cardinal number. He designated this smallest infinite cardinal number, $\aleph_0$, named "aleph-null"; aleph is a symbol in the Hebrew alphabet. He further showed that given any cardinal number, $\aleph_k$, there is a next smallest cardinal number, $\aleph_{k+1}$.

Cantor was able to prove that $|N| = \aleph_0$, and although many mathematicians believe that $|R| = \aleph_1$, this has never been proven from the axioms of mathematical set theory.

How Many Infinities?

- The theorem stated and proven next is due to Cantor and gives us a mechanism for defining two sets of distinctly different cardinality (one being strictly larger than the other). By inductively applying Cantor's theorem it follows that there are infinitely many cardinal numbers denoting the sizes of infinite sets. Cantor's theorem uses the power set of a given set.

Cantor's Theorem

Theorem (Cantor). Let S be any set. Then $|S| < |\mathcal{P}(S)|$.

Proof.

Case1: Suppose $S = \emptyset$. Then $\mathcal{P}(S) = \{\emptyset\}$. Since $|S| = 0$ and $|\mathcal{P}(S)| = 1$, the result holds.

Case2: Assume $S \neq \emptyset$.

(a) First we show that $|S| \leq |\mathcal{P}(S)|$.

To show this we must find an injection, f, from S to $\mathcal{P}(S)$.

Consider $f(x) = \{x\}$. Clearly, $f(x) \in \mathcal{P}(S)$ for all $x \in S$.

Furthermore, if $x \neq y$, then $f(x) = \{x\} \neq \{y\} = f(y)$.

Thus f is the desired function and we may conclude that $|S| \leq |\mathcal{P}(S)|$.

(b) Next we wish to show $|S| \neq |\mathcal{P}(S)|$. We do this by contradiction.

Assume $|S| = |\mathcal{P}(S)|$, then by definition of equality of cardinal numbers, there is a function, f, that is 1-1 and onto from S to $\mathcal{P}(S)$.

Define $Z = \{ x \in S \mid x \notin f(x) \}$. Clearly, Z is a subset (possibly empty) of S.

Therefore there is a $y \in S$ such that $f(y) = Z$. This follows from our assumption that f is onto $\mathcal{P}(S)$. Then either $y \in Z$ or $y \notin Z$.

(b.1) Suppose $y \in Z$, then by definition of Z, $y \notin f(y) = Z$; a contradiction.

(b.2) Suppose $y \notin Z$, then by definition of Z, $y \in f(y) = Z$; a contradiction.

Since the existence of f led to this logical absurdity, we must conclude that f cannot exist and thus $|S| = |\mathcal{P}(S)|$ is false. This establishes (b).

(a) and (b) together imply $|S| < |\mathcal{P}(S)|$.

Corollaries

- If $|S| = |N|$, then $|\mathcal{P}(S)| > |N| = \aleph_0$.

- There are sets whose cardinalities are greater than $\aleph_0$. These sets are uncountably infinite, whereas those that correspond to N are countably infinite.

- Note that a set can be countable and yet there is no effective way to describe its correspondence with N. Look back and you will see that the definition just says that an injective function **exists**, not that this function is actually **computable**.

Cardinalities of Z and Q

1. We show that $|N| = |Z|$.

   $|N| \leq |Z|$: Define **g:** $N \rightarrow Z$ as follows: **g(i) = i**

   $|Z| \leq |N|$: Define **f:** $Z \rightarrow N$ as follows:

$$f(x) = \begin{cases} 0 & , \text{if } x = 0 \\ 2x - 1, & \text{if } x > 0 \\ -2x & , \text{if } x < 0 \end{cases}$$

x=	0	1	-1	2	-2
f(x)=	0	1	2	3	4

2. To show $|N| = |Q|$ we develop the proof in two steps:

   (a) Lemma – prove that $|A| \leq |S|$ for every subset **A** of **S**.

   Note: This is what we did for $|N| \leq |Z|$

   (b) Prove that $|N \times N| = |N|$.

|Subset| $\leq$ |Parent Set|

Lemma A. $|A| \leq |S|$, for every subset **A** of **S**.

Proof. Let **A** be a subset of **S**. To establish that $|A| \leq |S|$ we need to find a 1-1 function from **A** into **S**. The identity function, **f(x) = x**, is the desired function; clearly, if $\mathbf{x} \neq \mathbf{y}$, then $\mathbf{f(x) = x \neq y = f(y)}$. Since $\mathbf{f(x)} \in \mathbf{S}$, for every **x** in **A**, the lemma is proved.

$| N \times N | = | N |$

Lemma B. $| N \times N | = | N |$.

Proof. Let **S** = $N \times N$ = **{(k,j) | k,j $\in N$}**. Define the function, f((k,j)) = ((k+j)(k+j+1))/2 + j.
Clearly f is a function, since the defining expression is single-valued.

Furthermore, $\forall$ k,j $\in$ N, f((k,j)) $\geq$ 0. We must show that f is 1-1 and onto N.
To show f is 1-1, let (k, j) and (k', j') be two distinct elements of S.
There are two cases to consider. (a) k+j = k'+j', or (b) k+j < k'+j' (or k'+j' < k+j).

Assume (a). Then f((k,j)) – f((k',j')) = j – j' (we can assume without loss of generality
that j-j' $\geq$ 0). If j-j' = 0, then j = j'. Thus k+j = k'+j' implies k = k', but this contradicts our
assumption that (k,j) and (k',j') are distinct elements of S. Thus, we must assume that
j-j' > 0. It follows immediately that f((k,j)) $\neq$ f((k',j')).

Assume (b).   Then we can assume k+j < k'+j' = k+j+a, for some a > 0. Now suppose
f(k',j')) = f((k,j)). Substituting k+j+a for k'+j' in the formula for f((k',j')) and equating to
f((k,j)), and doing the algebra we arrive at j = aj + y, where y is some positive number.
Clearly this relation cannot hold for any non-negative j and a > 0. We must conclude
that f((k,j)) $\neq$ f((k',j')). Thus, f is 1-1.

To show that f is onto N, we need to show that given any m $\geq$ 0, there is a (k,j) such
that f((k,j)) = m. Let x be the largest non-negative integer such that x(x+1)/2 $\leq$ m. It
follows that (x+1)(x+2)/2 > m. Now choose j = m - x(x+1)/2 and k = x-j.   It follows that
f((k,j)) = m.

Proof That $|N| = |Q|$

By definition, $Q = \{ (a,b) \mid a \in Z \text{ and } b \in Z^+ \}$

$|Q| \leq |N|$.
   $Q \subseteq Z \times N$. Thus $|Q| \leq |Z \times N|$ by Lemma A.
   But $|Z \times N| = |N \times N|$ using an argument similar to that
   showing $|Z| = |N|$. (Define g by g(a,b) = (f(a),b)) where f
   is the function used to map Z to N.)
   By Lemma B it follows that $|Q| \leq |N|$.
$|N| \leq |Q|$.
   Define f(a) = (a,1). This is a 1-1 mapping from N into Q,
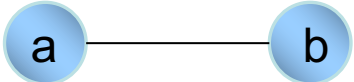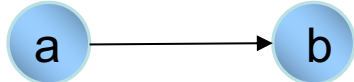   showing $|Q| \leq |N|$.

Thus, $|N| = |Q|$.

Undirected Graphs

- An **undirected Graph G** is defined by a pair **(V, E)**

- **V**: Finite Set of **Nodes/Vertices**

- **E**: { <a,b> | a,b∈**V** are called **Edges/Arcs**}
  - **E⊆V×V** such that <a,b>∈**E** implies <b,a>∈**E**

- **Degree** of node is number of edges at that node (number of nodes it relates to)

- Graphs can be **labeled**, as we did above on the nodes, or unlabeled.

- Labels can go on nodes, edges or both.

More on Graphs

- A **subgraph** H of a graph G is a subset of the nodes of G with all edges retained from G that involve node pairs in H.
- A **path** is a sequence of nodes connected by edges.
- A graph is **connected** if every two nodes are connected by a path.
- A **cycle** is a path that starts and ends in the same node.
- A **simple cycle** is a path that involves at least three nodes and starts and ends in the same node. (excludes self loop)
- A **tree** is a graph that is connected and has no simple cycles.
- A tree may contain a special node called the **root**.
- The nodes of degree 1 in a tree, excepting the root, are called **leaves**.
- The set of leaves of a tree are called the **frontier**.
- If the edges have direction then a graph is called **directed**

Directed vs Undirected

- If directed, we differentiate **in-degree** (edges into node) from **out-degree (edges out of node)**.

- Undirected (a)———(b)   Directed (a)——→(b)
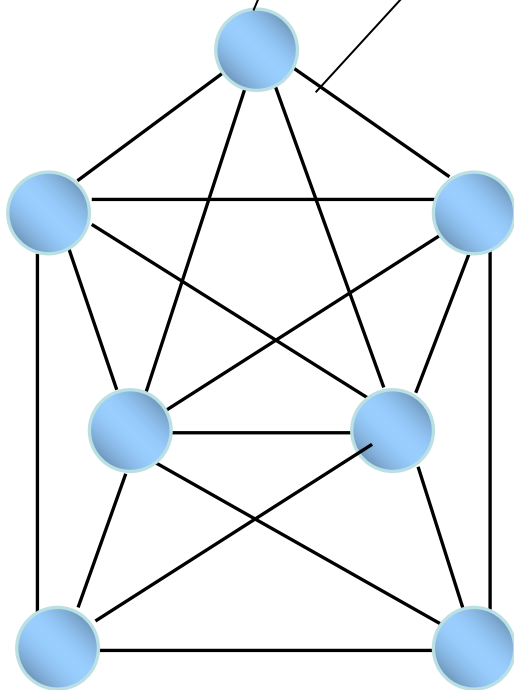
Graph G = (V, E)

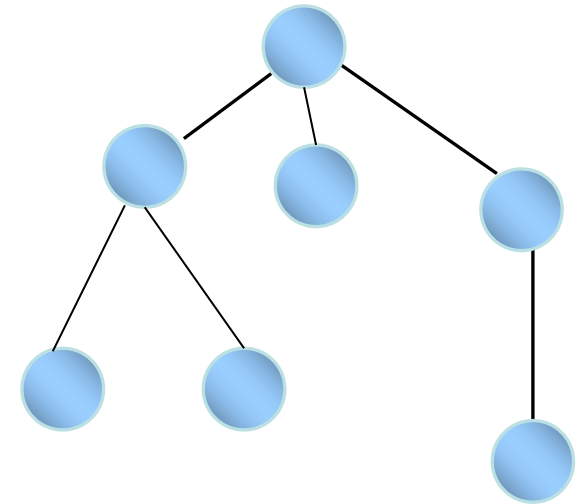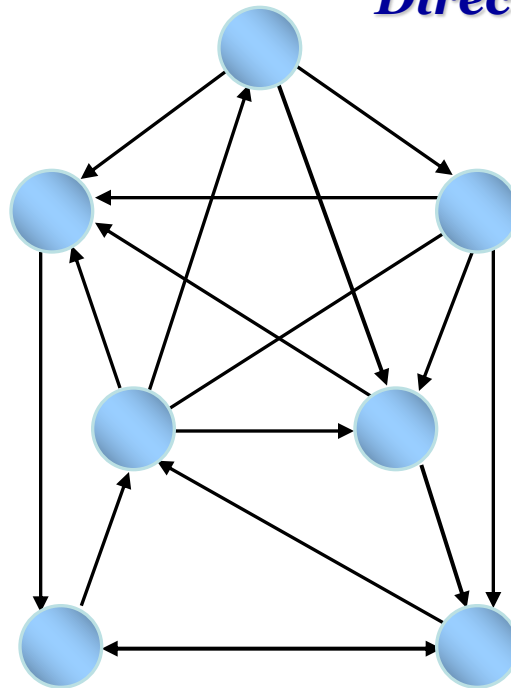*Undirected*

Nodes / Vertices

Edges / Arcs

V: Finite Set of Nodes/Vertices
E: $V \times V \rightarrow V$ are Edges/Arcs

Directed

$$(v_i, v_j) = (v_j, v_i)$$

Tree has no simple cycles and often has a root

Alphabets and Strings

- DEFINITION 1. An *alphabet* Σ is a finite, non-empty set of abstract symbols.
- DEFINITION 2. Σ^*, the set of <u>all strings over the alphabet, S</u>, is given inductively as follows.
  - Basis: $\lambda \in \Sigma^*$ (the *null string* is denoted by λ, it is the <u>string of length 0</u>, that is $|\lambda| = 0$) [many texts use ε but I avoid that as hate saying $\varepsilon \in A$; it's really confusing when manually written]
  $\forall a \in \Sigma$, $a \in \Sigma^*$ (the members of S are <u>strings of length 1</u>, $|a| = 1$)
  - Induction rule: If $x \in \Sigma^*$, and $a \in \Sigma$, then $a \cdot x \in \Sigma^*$ and $x \cdot a \in \Sigma^*$. Furthermore, $\lambda \cdot x = x \cdot \lambda = x$, and $|a \cdot x| = |x \cdot a| = 1 + |x|$.
  - *NOTE:* "$a \cdot x$" denotes "a *concatenated to* x" and is formed by appending the symbol a to the left end of x. Similarly, $x \cdot a$, denotes appending a to the right end of x. In either case, if x is the null string (λ), then the resultant string is "a".
  - We could have skipped saying $\forall a \in \Sigma$, $a \in \Sigma^*$, as this is covered by the induction rule with $x = \lambda$.

Languages

- DEFINITION 3. Let Σ be an alphabet. A *language over* Σ is a subset, L, of Σ^*.

- Example. Languages over the alphabet Σ = {a, b}.
  - Ø (the empty set) is a language over Σ
  - Σ^* (the universal set) is a language over Σ
  - {a, bb, aba } (a finite subset of Σ^*) is a language over Σ.
  - { $ab^n a^m$ | n = m^2, n, m $\geq$ 0 } (infinite subset) is a language over Σ.

- DEFINITION 4. Let L and M be two languages over Σ. Then the *concatenation of L with M*, denoted L·M is the set,
  L·M = { x·y | x $\in$ L and y $\in$ M }
  The concatenation of arbitrary strings x and y is defined inductively as follows.
  Basis: When $|x| \leq 1$ or $|y| \leq 1$, then x·y is defined as in Definition 2.
  Inductive rule: when $|x| > 1$ and $|y| > 1$, then x = x' · a for some a $\in \Sigma$ and x' $\in \Sigma^*$, where $|x'|$ = $|x|$-1. Then x·y = x'·(a·y).

Operations on Strings

- Let s, t be arbitrary strings over Σ
  - $s = a_1 a_2 \ldots a_j$, $j \geq 0$, where each $a_i \in \Sigma$
  - $t = b_1 b_2 \ldots b_k$, $k \geq 0$, where each $b_i \in \Sigma$
- length: $|s| = j$; $|t| = k$
- concatenate: $= s \cdot t = st =$
  $a_1 a_2 \ldots a_j b_1 b_2 \ldots b_k$; $|st| = j+k$
- power: $s^n = ss \ldots s$ (n times) Note: $s^0 = \lambda$
- reverse: $s^R = a_j a_{j-1} \ldots a_1$
- substring: for $s = a_1 a_2 \ldots a_j$, any $a_p a_{p+1} \ldots a_q$ where $1 \leq p \leq q \leq j$ or λ

Properties of Languages

- Let L, M and N be languages over Σ, then:
  - $\varnothing \cdot L = L \cdot \varnothing = \varnothing$
  - $\{\lambda\} \cdot L = L \cdot \{\lambda\} = L$
  - $L \cdot (M \cup N) = L \cdot M \cup L \cdot N$ and $(M \cup N) \cdot L = M \cdot L \cup N \cdot L$
    - Concatenation does **NOT** distribute over **intersection**.
  - $L^0 = \{\lambda\}$ (definition)
  - $L^{n+1} = LL^n = L^n L, n \geq 0$. (definition)
  - $L^+ = L^1 \cup L^2 \cup \dots L^n \dots$ (definition)
  - $L^* = L^0 \cup L^1 \cup L^2 \cup \dots L^n \dots$ (definition) $= L^0 \cup L^+$
  - $(L^*)^* = L^*$
  - $(LM)^* L = L(ML)^*$
  - $(L^* \cdot M^*)^* = (L^* \cup M^*)^* = (L \cup M)^*$
  - $(L^0 \cup L^1 \cup L^2 \cup \dots L^n) L^* = L^*$, for all $n \geq 0$.

Recognizers and Generators

1. When we discuss languages and classes of languages, we discuss recognizers and generators
2. A recognizer for a specific language is a program or computational model that differentiates members from non-members of the given language
3. A portion of the job of a compiler is to check to see if an input is a legitimate member of some specific programming language – we refer to this as a syntactic recognizer
4. A generator for a specific language is a program that generates all and only members of the given language
5. In general, it is not individual languages that interest us, but rather classes of languages that are definable by some specific class of recognizers or generators
6. One type of recognizer is called an automata and there are multiple classes of automata
7. One type of generator is called a grammar and there are multiple classes of grammars
8. Our first journey will be through automata and grammars

Terminology

- **Definitions** describe the mathematical objects and ideas we want to work with

- **Statements** or **assertions** are things we say about mathematics; they can be true or false

- **Proofs** are unassailable logical demonstrations that statements are true

- **Theorems** are statements that have been proven true

- **Lemmas** are theorems that are not interesting on their own but are useful for proving other theorems

- **Corollaries** are follow-on theorems that are easy to prove once you prove their parent theorems

Types of Proofs

- **Direct Argument**
  - Use assertions from theorem statement, known true properties and valid rules of inference
- **Construction**
  - Prove something exists by showing how to make it – a specific type of construction is a **reduction** (used frequently here to show one problem can be reduced to another)
- **Contradiction**
  - Prove something is true by showing it can't be false
  - One specific kind of proof by contradiction uses a technique called **diagonalization**

- **Weak Induction**
  - Show that a statement is true for some base case (often 0 or 1)
  - Show that *if* it's true for the case of some $i \geq$ base case, it's also true for the case of $i + 1$
- **Strong Induction**
  - Show that a statement is true for some base case (often 0 or 1)
  - Show that *if* it's true for all cases where $\leq i$, where $i \geq$ base case, it's true for the case of $i + 1$

Sample Proof by Induction

Prove, if n is a positive whole number and $n \geq 4$, then $2^n \geq n^2$. Hint: use induction with a base of n=4.

Proof by Induction:

Base Case: n = 4: $2^4 \geq 4^2$ since 16 ≥ 16.

Induction Hypothesis: Assume $2^k \geq k^2$, for some k ≥ 4.

Induction Step: Prove $2^{(k+1)} \geq (k+1)^2$

First, we observe that $k^2 \geq 2k+1$ when k ≥ 3.

   Consider k=m+1, where k ≥ 3; and so m ≥ 2

   $k^2 = (m+1)^2 = m^2 + 2m+1 \geq 4 + 2m+1 > 2m+3 = 2(m+1) + 1 = 2k+1$.

Using this,

$2^{(k+1)} = 2^k * 2 = 2^k+2^k \geq k^2 + k^2 \geq k^2 + 2k + 1 = (k+1)^2$

QED

Sample Proof by Contradiction

Prove, if p and q are distinct prime numbers, then $\sqrt{(p/q)}$ is irrational. Assume $\sqrt{(p/q)}$ is rational where p and q are distinct primes. Let a/b be the reduced fraction (no common prime factors) that equals $\sqrt{(p/q)}$.

$\sqrt{(p/q)} = a/b$: assumption (note a≠b, as p≠q)

$p/q = a^2/b^2$: square both sides

$p = a^2$ and $q = b^2$: since p and q have no common prime factors, and a and b have no common prime factors.

But this is not possible because p and q are prime numbers and so cannot have multiple factors (e.g., a × a, in the case of p). This contradicts our original assumption that $\sqrt{(p/q)}$ is rational, so it must be irrational. QED

Practice Problems

Practice

1. Prove or disprove that, for sets A and B,
   A=B if and only if $(A \cap \sim B) \cup (A \cap B) = A$.

2. Prove the following:
   For non-empty sets A and B, (AUB)=(A∩B) if and only if A=B
   What is the case is one or both are empty?

3. Prove: If S is any finite set with |S| = n, then
   $|S \times S \times S| \leq |P(S)|$, for all n≥N, where N is some constant, the minimum value of which you must discover and use as the basis for your proof.

4. Consider the function *pair*: $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$
   defined by *pair*(x,y) = $2^x(2y + 1) - 1$
   Show that *pair* is a bijection (1-1 onto $\mathbb{N}$).